

REMARKS

Reconsideration of the application is respectfully requested. An issue of public use on sale activity was raised. It is declared that the invention, including
5 Netseal's Mobile Network Product and RoamMate 2.1, was not described in a printed publication in the United States or in a foreign country or in public use or on sale in the United States more than one year prior to the date of application for patent in the United States.

10 The abstract was objected to for being non-conforming and too long. The abstract has been revised and should now be in full conformance. No new matter has been added.

15 Claims 3-4, 7 and 12-13 were objected to. The claims have now been corrected and should be in full conformance. No new matter has been added.

Claims 1-20 were rejected under Section 102 as being anticipated by Makineni. This rejection is respectfully traversed. The amended claims include no new matter.

20 To summarize the present invention, it is an effective method for sending messages over secure communication links when a mobile terminal moves from an initial network address to a new network address without having to use complicated key interchange protocols when
25 setting up the new communication link. It solves the problem of sending messages from the new network address although there are unknown intermediate computers (NAT) that may translate, when the new address is not supported, and even block messages. The terminals send encapsulated messages that
30 overcome network translations by intermediate computers while conforming to encapsulation methods that are supported by the receiving terminal. More particularly, a first secure communication link is established between a first terminal, located at an initial network address, and a second terminal.
35 The first terminal sends encapsulated messages using a first

encapsulation method. The first terminal moves to a new network address. The first terminal sends an encapsulated request message using the first encapsulation method to change the communication to be in a second secure communication link of the new network address. The second terminal receives the request message and detects any translations made en route by intermediate computers. The second terminal sends back a reply message with a description of the translations made and encapsulation methods supported by the second terminal. The first terminal receives the reply message and selects an encapsulation method based on the information in the reply message for future messages sent in the second secure communication link.

These steps ensure that future messages from the new address are encapsulated in a way that are both supported by the second terminal and are not translated or even blocked by any intermediate computers.

Makineni merely describes communication between a mobile terminal and its home server when the mobile terminal roams outside of the home network. In Fig. 2, the client 24 sends an encapsulated via an encrypted tunnel 20 to the home server 14. At step 105, the home server 14 merely registers the new IP address of the client 24 (see paragraphs [0027-0028]). At step 106, the server 14 transmits a reply message to the client confirming the registration of the new IP address and a security association is formed between the client and the home server.

Makineni fails to teach or suggest the steps of the client performing encapsulation of messages sent in the first secure communication link using a first encapsulation method i.e. prior to roaming outside the home network. In other words, this is when client 16 is located within the home network 12 and directly linked to the home server 14 via connection 18 (see Fig. 1 and paragraph [0026]). It is submitted that Makineni completely fails to teach or suggest

the client 16 sending encapsulated messages to the server while inside the home network 12. Applicants fail to see that there is any motivation to modify Makineni to include the step of the client 16 sending encapsulated messages while being in
5 the home network 12 since the address of client 16 is, almost by definition, known. It is submitted that an artisan would know that no encapsulation is needed when sending messages within the home network. It is therefore submitted that it would not be obvious and it would not make sense to modify
10 Makineni so that the client 16 sends encapsulated messages, using the first encapsulation method, to the home server 14 while they are inside the same home network 12.

Consequently, Makineni also fails to teach or suggest the step of the first terminal sending an encapsulated
15 request message from the new network address using the same encapsulation method when sending in the first secure communication link since no encapsulation method was used in the first secure communication link 18 (see Figs. 1-2).

Makineni also fails to teach or suggest the
20 encapsulated request message including a description of the first encapsulation method. Makineni's request message seems only contain the new IP address but there is no description of the first encapsulation method included in the request message.

More importantly, Makineni's home server 14 never
25 uses the description of the first encapsulation method to detect any translations made by intermediate computers. As a result, Makineni also fails to teach including in the reply message a description of the detected translations and
30 encapsulation methods supported by the home server. In contrast, at step 106, the home server 14 transmits a reply message to the client confirming the registration of the new IP address (see paragraph [0027]). There is no teaching about the home server 14 detecting translations performed by
35 intermediate computers. Additionally, the reply message does

not include encapsulation methods supported by the home server 14.

5 Makineni fails to teach or suggest the first terminal selecting an encapsulation method, when sending from the new network address, that is based on the description in the reply message about translations made by intermediate computer and encapsulation methods supported by the home server 14.

10 Makineni fails to address the problem of intermediate computers performing undesirable translations when the mobile terminal moves to a new address. Makineni merely discusses the same firewall and VPN gateways of the home network which of course are all known. Makineni therefore does not include anything about the idea of including a description of the encapsulation method in the request message so that the receiving terminal can determine whether intermediate NAT devices, on the route, have manipulated the message or not. Makineni also fails to use this information in the reply message so that the mobile terminal can select an encapsulation method that overcome both translations by intermediate NAT devices while conforming to encapsulation methods supported by the home server.

25 It is submitted that Makineni requires extensive modifications that are not taught or suggested to meet all the requirements of the amended claims. Applicants fail to see why a person of ordinary skill in the art would look to Makineni to learn about the steps in the amended claim 1 when such steps are completely missing in Makineni, as described above.

30 In view of the above, it is submitted that the amended claim 1 is not anticipated nor rendered obvious by Makineni. It is therefore submitted that the amended claim 1 is allowable.


35 Claims 2-20 are submitted to be allowable because they depend upon the allowable base claim 1 and because each

claim includes limitations that are not taught or suggested in the cited references.

The application is submitted to be in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

FASTH LAW OFFICES



Rolf Fasth
Registration No. 36,999

Attorney reference number: 290.1075USN

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301
Telephone: (910) 687-0001
Facsimile: (910) 295-2152
Email: rolf.fasth@fasthlaw.com

cc: Lisbeth Soderman, Iprbox Ltd.
(Your ref: S0053US)